



## Was ist Informationssicherheit – Grundlagen, Ziele & Maßnahmen

Informationssicherheit und ein wirksames Informationssicherheitsmanagement gehören heute zu den wichtigsten Aufgaben jeder modernen Organisation. Die VOREST AG unterstützt Sie dabei mit langjähriger Erfahrung und praxisnahen Lösungen. In einer digital vernetzten Welt gehören Informationen und Daten zu den wichtigsten Ressourcen, deren Schutz ein entscheidender Erfolgsfaktor ist. Datenschutz und Informationssicherheit greifen dabei eng ineinander und bilden die Grundlage für Vertrauen und nachhaltigen Geschäftserfolg.

Informationssicherheit bedeutet weit mehr als nur klassische IT-Sicherheit. Sie umfasst technische, organisatorische und personelle Maßnahmen, um Informationen ganzheitlich vor Risiken wie Manipulation, Ausfall oder Diebstahl zu schützen. Dazu gehören unter anderem klare Prozesse, Schulungen für Mitarbeiter sowie moderne Sicherheitslösungen.

**Setzen Sie auf Erfahrung:** Die VOREST AG begleitet Sie mit den passenden Weiterbildungen seit Jahren erfolgreich in den Bereichen Informationssicherheit und ISO 27001. [Hier erfahren Sie mehr über unsere ISO 27001 Schulungen >>](#)

### Was bedeutet Informationssicherheit?

Informationssicherheit beschreibt den Schutz von Informationen und Daten vor unbefugtem Zugriff, Manipulation, Verlust oder Diebstahl. Ziel ist es dabei, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen dauerhaft zu gewährleisten. Dazu werden technische Maßnahmen, organisatorische Prozesse sowie klare Richtlinien eingesetzt. Ebenso entscheidend ist die Sensibilisierung der Mitarbeiter, da menschliche Fehler zu den häufigsten Ursachen für Sicherheitsvorfälle zählen.

Besonders wichtig ist Informationssicherheit für Organisationen, die mit sensiblen Daten arbeiten, etwa personenbezogene Daten, geistigem Eigentum oder finanziellen Daten. Ein wirksames Management der Informationssicherheit stärkt nicht nur die Widerstandsfähigkeit gegen Sicherheitsvorfälle, sondern auch das Vertrauen von Kunden, Partnern und Mitarbeitern.

Unternehmen sehen sich dabei vielfältigen Bedrohungen ausgesetzt: von Fahrlässigkeit und Betrug über Spionage und Vandalismus bis hin zu Naturgefahren wie Feuer oder Hochwasser. Die Informationssicherheit hilft dabei, diese Risiken zu reduzieren oder ganz zu vermeiden.

## Video – Was ist Informationssicherheit?

In der digitalen Welt sind Informationen zu einem der wertvollsten Vermögenswerte geworden. Unternehmen sammeln und verarbeiten riesige Datenmengen. Deshalb ist es von entscheidender Bedeutung, dass diese Informationen sicher und geschützt sind. In diesem Video erfahren Sie mehr darüber, was Informationssicherheit ist und wie wertvolle Daten geschützt werden können. Außerdem erhalten Sie einen Überblick über die Schutzziele der Informationssicherheit.

### Inhalte:

- Betrachtung der Informationen als Vermögenswerte
- Unterteilung der Schutzziele
- Informationssicherheitsrisiko



## Warum ist Informationssicherheit wichtig?

Informationssicherheit ist wichtig, weil sie den wachsenden Wert von Daten schützt. Ob Kundendaten, Forschungsunterlagen oder Geschäftsstrategien, ein Verlust oder Missbrauch kann enorme finanzielle Schäden verursachen und das Vertrauen in ein Unternehmen nachhaltig schädigen.

### Häufige Ursachen für Sicherheitsvorfälle sind:

- Cyberangriffe & Ransomware
- Menschliche Fehler
- Veraltete IT-Systeme & Software
- Unklare Prozesse oder organisatorische Schwächen

Die Folgen reichen von Reputationsverlust und Produktionsausfällen bis hin zu hohen Kosten durch Rechtsverstöße (z. B. bei Nichteinhaltung der [DSGVO – Datenschutz-Grundverordnung](#)).

→ Deshalb ist Informationssicherheit unverzichtbar: Sie schützt sensible Daten, reduziert Risiken und stellt sicher, dass Organisationen rechtskonform, handlungsfähig und wettbewerbsfähig bleiben.

## Was sind die Schutzziele der Informationssicherheit?

Die Schutzziele der Informationssicherheit beschreiben die grundlegenden Sicherheitsanforderungen an Daten und Systeme. Sie bilden die Basis jedes Informationssicherheitsmanagementsystems (ISMS) nach [ISO 27001](#). Die drei zentralen Schutzziele sind Vertraulichkeit, Integrität sowie Verfügbarkeit.

### Vertraulichkeit

Informationen dürfen nur von autorisierten Personen oder Prozessen eingesehen werden. Unbefugter Zugriff, ob absichtlich oder versehentlich, muss durch Zugriffskontrollen, Berechtigungskonzepte und Verschlüsselung verhindert werden.

**Beispiel:** Nur Mitarbeiter der Personalabteilung dürfen auf Gehaltsdaten zugreifen; der Zugriff ist durch Passwörter und Rollenrechte abgesichert.

### Integrität

Daten und Systeme müssen richtig, vollständig und unverfälscht bleiben. Veränderungen durch Manipulation oder Fehler können die Integrität zerstören, etwa durch falsche Angaben zum Autor, eine unerlaubte Bearbeitung oder manipulierte Zeitstempel.

**Beispiel:** Ein digitales Vertragsdokument wird mit einer elektronischen Signatur versehen, sodass jede nachträgliche Änderung sofort erkennbar wäre.

### Verfügbarkeit

Informationen und Systeme müssen zum richtigen Zeitpunkt für befugte Nutzer zugänglich sein. Systemausfälle oder Angriffe können Prozesse lahmlegen. Unternehmen müssen daher kritische Systeme besonders gegen Ausfälle und Störungen absichern.

**Beispiel:** Ein Online-Shop setzt auf regelmäßige Backups und Notfall-Server (Redundanz), damit Kunden auch bei einem Serverausfall weiterhin einkaufen können.

## Schutzziele der Informationssicherheit im ISMS

### SCHUTZZIELE



#### Verfügbarkeit

Dem Benutzer stehen Dienstleistungen, Funktionen eines IT-Systems oder auch Informationen zum geforderten Zeitpunkt zur Verfügung.



#### Integrität

...bedeutet zum einen die Richtigkeit und Vollständigkeit der verarbeiteten Daten/Information und zum anderen die korrekte Funktionsweise der Systeme. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert wurden oder Angaben zum Autor verfälscht wurden oder der Zeitpunkt der Erstellung manipuliert wurde.



#### Vertraulichkeit

Schutz der Systeme und Daten vor unberechtigtem Zugriff durch Personen oder Prozesse.

Übersicht über die drei zentralen Schutzziele der Informationssicherheit innerhalb eines Informationssicherheitsmanagementsystems mit Beschreibung für jedes Schutzziel.

## Was ist Informationssicherheitsmanagement?

Ein wirksames Informationssicherheitsmanagement ist kein einmaliges Projekt, sondern ein fortlaufender Prozess und umfasst alle organisatorischen, technischen sowie personellen Maßnahmen, um Informationssicherheit im Unternehmen systematisch zu planen, umzusetzen und kontinuierlich zu verbessern.

## Ziele des Informationssicherheitsmanagements

Die Ziele lassen sich nicht auf einzelne Maßnahmen reduzieren. Sie bilden den strategischen Rahmen, um Informationsrisiken nachhaltig zu steuern und rechtliche wie organisatorische Anforderungen zu erfüllen:

- Risiken systematisch identifizieren und bewerten
- Sicherheitsziele definieren und geeignete Maßnahmen umsetzen
- Regelmäßige Audits und kontinuierliche Verbesserungen etablieren
- Compliance mit Normen und Gesetzen sicherstellen
- Verantwortlichkeiten und Zuständigkeiten klar regeln und dokumentieren
- Mitarbeiter regelmäßig sensibilisieren und schulen, um Risiken frühzeitig zu erkennen.

## Das Informationssicherheitsmanagementsystem (ISMS)

Ein [Informationssicherheitsmanagementsystem \(ISMS\)](#) ist das zentrale Instrument, um Informationssicherheit im Unternehmen strukturiert umzusetzen. Es bietet ein Rahmenwerk, mit dem Organisationen ihre Sicherheit systematisch steuern, überwachen und kontinuierlich verbessern können. Auch das [BSI](#) betont die Bedeutung von Managementsystemen wie dem ISMS für den Schutz sensibler Informationen.

Die ISO/IEC 27001 ist sicherlich die wichtigste Norm im Bereich der Informationssicherheit. Sie definiert Anforderungen an ein ISMS und legt fest, wie Informationssicherheit geplant, umgesetzt, geprüft und kontinuierlich verbessert werden muss.

### Merkmale eines ISMS:

- Risikobasierter Ansatz zur Identifizierung und Bewertung von Bedrohungen
- Regelkreismodell (Plan-Do-Check-Act) für kontinuierliche Verbesserung
- Integration in bestehende Unternehmensprozesse statt isolierter Insellösungen
- Orientierung an ISO/IEC 27001, dem international anerkannten Standard für Informationssicherheit







Nach erfolgreicher Einführung können Unternehmen ihr ISMS nach ISO 27001 zertifizieren lassen. Eine [ISO 27001 Zertifizierung](#) durch eine akkreditierte Stelle signalisiert Kunden, Partnern und Behörden ein hohes Maß an Sicherheitsbewusstsein und Professionalität im Bereich [Datenschutz](#) und Informationssicherheit.

## Ihre ISMS Schulungen bei der VOREST AG – Die Basis für ein erfolgreiches Informationssicherheitsmanagement


Ein erfolgreiches Informationssicherheitsmanagement lebt von Wissen. Mit unseren [Schulungen im Bereich der ISO 27001](#) qualifizieren Sie sich zu allen Anforderungen eines erfolgreichen ISMS. Wir bieten Ihnen praxisnahe Weiterbildungen zur Einführung eines ISMS, zur Tätigkeit als interner Auditor, ISMS-Beauftragter oder externer Auditor nach ISO/IEC 27001. Unsere Trainings vermitteln praxisnahes Know-how, unterstützen bei der Einhaltung von Norm-Anforderungen und fördern die Awareness im Unternehmen. Kurzum, unsere Ausbildungen machen Sie fit, Informationssicherheit systematisch umzusetzen, Risiken zu minimieren und Ihr Unternehmen nachhaltig abzusichern. Damit bereitet die VOREST AG Sie optimal auf Ihre Aufgaben im Bereich der Informationssicherheit vor.

Sie wünschen sich ein maßgeschneidertes Seminar zur IT-Sicherheit oder spezifischen Prozessen in Ihrem Unternehmen? Mit unseren [Inhouse Schulungen ISO 27001](#) kommen wir zu Ihnen und schulen Sie zu Ihrem Wunschthema.

Gerne stehen wir Ihnen auch [beratend zur Seite](#) – sprechen Sie uns einfach an.


	<p><b>Kostenloser E-Learning Kurs - Was ist ein ISMS nach ISO 27001?</b></p> <p>Kostenloser E-Learning Kurs zum Informationssicherheitsmanagement mit erstem Überblick über die Bedeutung eines ISMS sowie über die Funktionsweise und Ziele der Norm ISO 27001.</p> <p>Preis: 0,00 €   Kursformat: E-Learning</p>	<a href="#">zum Kurs »</a>
	<p><b>Basiswissen ISMS ISO 27001</b></p> <p>Grundlagen Kurs zu den Inhalten und Forderungen der Norm DIN EN ISO/IEC 27001 für Informationssicherheitsmanagementsysteme und zur Einführung &amp; Zertifizierung eines ISMS.</p> <p>Preis: 1099,00 €   Kursformat: Präsenz   Preis: 1044,05 €   Kursformat: Virtual-Classroom</p>	<a href="#">zum Kurs »</a>
	<p><b>Interner Auditor ISO 27001</b></p> <p>Schulung zur Vorbereitung, Durchführung und Nachbereitung von internen Audits nach ISO 19011 im Informationssicherheitsmanagementsystem nach ISO 27001 - <b>Abschluss mit Zertifikat.</b></p> <p>Preis: 1099,00 €   Kursformat: Präsenz   Preis: 1044,05 €   Kursformat: Virtual-Classroom</p>	<a href="#">zum Kurs »</a>
	<p><b>Informationssicherheitsbeauftragter - ISMS Beauftragter ISO 27001</b></p> <p>Ausbildung zur Rolle und den Aufgaben des ISMS-Beauftragten ISO 27001 mit Qualifikation zur Betreuung &amp; Weiterentwicklung eines Informationssicherheitsmanagementsystems - <b>Abschluss mit Zertifikat.</b></p> <p>Preis: 1299,00 €   Kursformat: Präsenz   Preis: 1234,05 €   Kursformat: Virtual-Classroom</p>	<a href="#">zum Kurs »</a>
	<p><b>Informationssicherheitsmanagement Auditor / Leitender Auditor ISO 27001</b></p> <p>Ausbildung zum Erwerb des fachlichen und persönlichen Know-how zur Durchführung externer Audits und Zertifizierungsaudits im ISMS als (Lead) Auditor ISO 27001 - <b>Abschluss mit Zertifikat.</b></p> <p>Preis: 2399,00 €   Kursformat: Präsenz   Preis: 2279,05 €   Kursformat: Virtual-Classroom</p>	<a href="#">zum Kurs »</a>
	<p><b>Kostenloser Gesamtkatalog der VOREST AG zum Download</b></p> <p>Gesamtkatalog der VOREST AG mit allen Schulungen rund um Managementsysteme, Prozessoptimierung und Methoden zum kostenlosen Download.</p>	<a href="#">Download »</a>

Sie wissen noch nicht, welcher Kurs der richtige ist?  
Fragen zu Formaten, Förderung oder Inhalten?



Sevil Kaya

**Sevil Kaya**  
Mail: [skaya@vorest-ag.de](mailto:skaya@vorest-ag.de)  
Telefon: 07231 92 23 91 33



Katharina Reutter

**Katharina Reutter**  
Mail: [kreutter@vorest-ag.de](mailto:kreutter@vorest-ag.de)  
Telefon: 07231 92 23 91 37

## Normen und Standards im Informationssicherheitsmanagement

Um Informationssicherheit wirksam und nachvollziehbar umzusetzen, orientieren sich Unternehmen an anerkannten Normen und Standards. Diese bieten praxisnahe Leitlinien für den Aufbau eines Informationssicherheitsmanagementsystems (ISMS) und schaffen die Grundlage für eine einheitliche Bewertung und Zertifizierung.

### Wichtige Normen und Standards im Überblick:

- **ISO/IEC 27001** – internationaler Standard für den Aufbau und Betrieb eines ISMS
- **ISO/IEC 27002** – Leitfaden für konkrete Sicherheitsmaßnahmen
- **BSI IT-Grundschutz**
- **NIS-2** – EU-Richtlinie für kritische Infrastrukturen und Unternehmen von besonderer Bedeutung
- **DSGVO** – Datenschutzanforderungen mit engem Bezug zur Informationssicherheit

## Video – Standards der ISMS ISO/IEC 27000 Reihe

Die Informationssicherheit wird in der heutigen Zeit immer wichtiger und Unternehmen müssen sicherstellen, dass ihre Daten und Systeme vor Bedrohungen geschützt sind. Einen auf international anerkannten Standards basierenden Rahmen dafür bildet die ISO/IEC 27000 Reihe.

In diesem Video erhalten Sie einen Überblick über die wichtigsten Standards der ISO/IEC 27000 Reihe und wie sie Unternehmen helfen können ihre Informationssicherheit zu verbessern.

### Inhalte dieses Videos:

- Bestandteile der ISO 27001
- Bestandteile der ISO 27006
- Bestandteile weiterer informativer Normen
- Begriffsnorm – Abschnitt 5.2
- Anforderungsnormen – Abschnitt 5.3
- Leitfadennormen – Abschnitt 5.4
- Sektorenspezifische Leitfadennormen – Abschnitt 5.5
- Maßnahmenbezogene Leitfadennormen



## Welche Bedeutung hat die ISO 27001 im Informationssicherheitsmanagementsystem?

Bei der [DIN EN ISO/IEC 27001](#) handelt es sich um eine internationale Norm, die Unternehmen bei der Gewährleistung der Informationssicherheit unterstützt. Sie legt die Anforderungen an die Einführung, den Betrieb und die kontinuierliche Verbesserung eines ISMS fest. Ziel ist es, Informationssicherheit systematisch zu managen und an die individuellen Bedürfnisse einer Organisation anzupassen.

Unternehmen können die ISO 27001 sowohl als Leitfaden für den Aufbau eines ISMS als auch als Grundlage für eine Zertifizierung nutzen. Für eine Zertifizierung durch eine akkreditierte Stelle müssen alle in der Norm definierten Anforderungen erfüllt sein.

## Video – Was ist die ISO 27001 und deren Anforderungen?

Die ISO/IEC 27001 ist die international führende Norm für das Informationssicherheitsmanagement. Sie definiert die Anforderungen an ein Informationssicherheitsmanagementsystem (ISMS) und spielt eine zentrale Rolle beim Schutz sensibler Daten und Informationen in Unternehmen weltweit. Ziel der Norm ist es, Informationssicherheitsrisiken systematisch zu erkennen, geeignete Maßnahmen umzusetzen und die Sicherheit kontinuierlich zu verbessern.

In diesem Video erfahren Sie, welche Anforderungen die ISO 27001 stellt, wie ein ISMS aufgebaut sein muss und warum eine Zertifizierung nach ISO 27001 für Organisationen von Vorteil sein kann.

### Inhalte des Videos:

- Was ist die ISO 27001?
- Inhalte und Anforderungen der ISO 27001
- Zertifizierung des ISMS



## Welche Rolle spielt die Statement of Applicability in der ISO 27001?

Die Statement of Applicability (SoA) ist ein zentrales Element eines jeden ISMS nach ISO 27001. Sie listet alle möglichen Sicherheitsmaßnahmen aus Anhang A auf und dokumentiert, welche Controls für das jeweilige Unternehmen relevant sind, wie sie umgesetzt werden und warum bestimmte Maßnahmen ausgeschlossen wurden. Damit ist die SoA nicht nur ein Nachweis für Audits und Zertifizierungen, sondern auch ein wichtiges Werkzeug im Risikomanagement, da sie zeigt, mit welchen Maßnahmen Informationssicherheitsrisiken systematisch gemindert werden.

## Video zur ISO 27002 und deren Anforderungen

Die ISO 27002 ist eine internationale Norm, die als Best-Practice-Leitfaden für Informationssicherheit dient. Das heißt, sie liefert konkrete Umsetzungsmaßnahmen für die in der ISO 27001 geforderten Maßnahmen.

In diesem Video der VOREST AG erfahren Sie welche Anforderungen die Norm ISO 27002 stellt und wozu sie genau da ist. Zudem lernen Sie, welchen Zweck die Norm verfolgt und inwiefern sie in Ihrem Unternehmen verpflichtend ist.

### Inhalte dieses Videos:

- Umsetzungshilfen zu den Anforderungen der ISO 27001
- Ist die ISO 27001 verpflichtend?



## Informationssicherheit vs. Datenschutz vs. IT-Sicherheit

Informationssicherheit, Datenschutz und IT-Sicherheit werden häufig verwechselt, unterscheiden sich jedoch deutlich in ihrem Fokus und Anwendungsbereich. Die folgende Tabelle zeigt die Unterschiede und Schwerpunkte der drei Begriffe auf einen Blick:

Begriff	Fokus	Beispiel
<b>Informationssicherheit</b>	Ganzheitlicher Schutz aller Informationen (digital & analog)	Zugriffskontrollen, Sicherheitsrichtlinien, Notfallmanagement
<b>Datenschutz</b>	Schutz personenbezogener Daten, gesetzliche Vorgaben (DSGVO)	Speicherung von Kundendaten nur mit Einwilligung
<b>IT-Sicherheit</b>	Technischer Schutz von IT-Systemen, Netzwerken und Geräten; Funktionssicherheit	Firewalls, Backups, Virens Scanner

**Fazit:** Während Datenschutz und IT-Sicherheit jeweils Teilbereiche sind, integriert die Informationssicherheit beide Perspektiven in ein übergeordnetes, umfassendes Schutzkonzept. Dies passiert häufig im Rahmen eines Informationssicherheitsmanagementsystems (ISMS).

## Zukunft der Informationssicherheit

Das große Stichwort lautet: **KI**. Die Zukunft der Informationssicherheit und Cybersecurity wird zunehmend von KI, automatisierten Angriffen und strengeren Regulierungen geprägt. Angreifer setzen zunehmend auf KI-gesteuerte Phishing-Angriffe, Deepfakes und Schadsoftware ([Google Threat Intelligence 2025](#)).

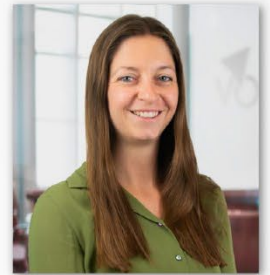
Aktuelle Analysen, wie etwa von [McKinsey](#) zeigen: KI ist zugleich die größte Bedrohung und die stärkste Verteidigung in der Cybersecurity. Während Angreifer KI nutzen, um Angriffe realistischer, schneller und schwerer erkennbar zu machen, eröffnet dieselbe Technologie enorme Chancen für Unternehmen, ihre Abwehr zu stärken.

**Für Unternehmen bedeutet das:** Investieren Sie jetzt in proaktive Sicherheitsstrategien und schulen Sie Ihre Mitarbeiter, um auf die kommende Entwicklung in der Informationssicherheit vorbereitet zu sein.

■ **Sie haben Fragen oder wünschen ein Angebot?**  
Ich helfe Ihnen gerne weiter!

**Kati Schäfer**  
Produktmanagement Training & PRO SYS

☎ 07231 92 23 91 - 0  
✉ [kschaefer@vorest-ag.de](mailto:kschaefer@vorest-ag.de)



■ **Inhouse Training – Wir kommen zu Ihnen ins Haus!**  
Sie wünschen ein Angebot?

**Claudia Talmon**  
Produktmanagement Training

☎ 07231 92 23 91 - 0  
✉ [ctalmon@vorest-ag.de](mailto:ctalmon@vorest-ag.de)



## Unser Katalog für 2025

Laden Sie hier kostenfrei und unverbindlich unseren **Katalog** mit einer Übersicht zu allen unseren aktuellen **Schulungen** und **E-Learning-Kursen** herunter.

